DOE HSPD-12 FAQ (V4)

SCOPE AND DEFINITIONS

1. What is HSPD-12?

HSPD-12 is a Presidential Policy signed Aug 27, 2004. It:

- Requires background investigations (BI) on all federal and contractor employees.

- Requires a new security badge to be a smartcard which will be used to access Federally owned or leased facilities and to access federal computer systems.

- Directed Department of Commerce (via National Institute of Standard and Technology) to issue the technical requirements.

- Directed OMB to issue clarifying guidance.

2. What is FIPS 201?

FIPS 201 is the Standard created by NIST on HSPD-12.

3. Where can I get a copy of all of these documents?

Many of these public documents are available on the CIO web site, http://cio.doe.gov/HSPD-12/index.html.

4. What are the HSPD-12 timelines?

- After October 27, 2005, agencies will only issue a badge to a new federal or contractor employee after a BI and begin BIs on existing staff. The badge issued will be the current DOE badge.

- After October 27, 2006, agencies will only issue smartcards as badges (note that DOE will start to issue smartcards around the Spring of 2006).

- After October 27, 2007 all federal and contractor employees must have and use their smartcard.

5. What is PIV?

PIV stands for Personal Identity Verification.

6. What is PIV-I and PIV-II?

FIPS 201 has 2 parts: PIV-I and PIV-II. PIV-I deals with performing background checks for employees and contractors. PIV-II deals with issuing smartcards.

7. The term credential is used in HSPD-12 and FIPS 201. Is a credential different from a DOE badge?

For this purpose the term credential means a DOE Security Badge.

8. What are the Department's badging requirements to meet PIV-I?

PIV-I badges can only be issued to new employees and contractors after the identity proofing process has occurred.

9. What is a PIV-I badge/credential?

For PIV-I, it is the credential issued for long term access to Federal resources after identity proofing has been completed.

10. Can a current Science or other approved DOE badge be issued?

For PIV-I, the badge that currently exists will be used, but the identity proofing requirement must be met before issuance. Under PIV-II, the Smartcard will become the DOE badge.

11. What if my activity does not currently issue badges?

The requirement still exists for conducting background checks on new employees and contractors.

12. How will sites that have no previous experience working with OPM to conduct background checks ensure such checks are conducted?

Sites with no current experience will have to affiliate themselves with DOE Federal sites and Registrars that currently perform this function.

13. Who requires a PIV credential?

People with long term access to Federal resources.

14. Does this apply to contractors, visitors, detailees, assignees, and foreign nationals?

Yes, if they require long term access to Federal resources.

15. What is long term access?

Greater than 6 consecutive months.

16. What is short term access?

Less than 6 consecutive months.

17. What about people who require intermittent access?

If the person is expected to required access for longer than 6 consecutive months, then a PIV badge is needed.

18. Can a site issue a short term badge while the PIV badge is pending?

Yes.

19. Can a site use the identity proofing process for short term badges?

Yes.

20. What is DOE Notice 206.1?

This is the directive that identifies implementation requirements of PIV-I within the Department of Energy. This Notice requires personnel identification to be based upon sound criteria for verifying an individual's identity prior to being issued a DOE badge.

21. **OMB guidance requires Privacy Impact Assessments to protect personal information. How is this requirement going to be implemented within the Department of Energy?**

    DOE will adhere to all required privacy legislation and regulations.

22. **What is the criterion to be used to adjudicate the background investigations for contractor or federal employees who require an HSPD-12 badge but who will not receive an access authorization?**

    The initial criterion is (1) is, or is suspected of being, a terrorist; (2) is the subject of an outstanding warrant; (3) has deliberately omitted, concealed, or falsified relevant and material facts from any Questionnaire for National Security Positions (SF-86), Questionnaire for Non-Sensitive Positions (SF-85), or similar form; (4) has presented false or forged identity source documents; (5) has been barred from Federal employment; or (6) is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or (7) is awaiting or serving a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

23. **Does DOE Notice 206.1 pertain to both physical and logical access?**

    No. This PIV-I Notice addresses only physical access.

IDENTITY PROOFING PROCESS

1. **What is the difference between a NAC and a NACI?**

    The following describes the details of a National Agency Check (NAC) and a National Agency Check with Inquiries (NACI).

    The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check.

    NACI. The investigation consists of a NAC with written inquiries and searches of records covering specific areas of an individual's

background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes:

- Employment, 5 years

- Education, 5 years and highest degree verified

- Residence, 3 years

- References

- Law Enforcement, 5 years

2. **Processing a NACI can take a long time, what do we do in the meantime?**

    The NACI is initiated for the background investigation. A PIV credential can be issued after the results of the NAC (National Agency Check) are known. If, however, the results of the NAC are not received in 5 days, the credential can be issued based on the FBI National Criminal History Check (fingerprint check).

3. **If the FBI fingerprint does not come back in 5 days, can the badge be issued?**

    No. However, the individual could be considered short-term and handled under those procedures.

4. **Can the NACI for access authorization (security clearance) be used to satisfy the PIV identity proofing process?**

    Yes.

5. **How does PIV relate to the access authorization (security clearance) process?**

    They are two separate processes.

6. **What if the NACI is several years old, from a different agency, or is from a clearance at a previous agency?**

    As long as the completed NACI can be verified, the credential can be issued.

7. **PIV-I applies to new employees and contractors, how is identity proofing done for current employees and contractors?**

    A plan is being developed to satisfy the requirement that all current employees and contractors have completed background investigations by October 27, 2007.

    Since Federal personnel records are usually kept for only 15 years, a NACI may not have remained on record for some Federal employees. There is an allowance that background investigations for all Federal employees employed for over 15 years have until October 2008 to be completed.

8. **Can contractors who have been employed by the Department for over 15 years be included during the "grace period"?**

No provision is made for this.

9. **Can replacement badges be issued to current employees and contractors without the identity proofing process?**

Yes.

10. **If a contract changes, but the person/people remain doing the DOE work, does the background check have to be done?**

If the same person/people were previously employed on a DOE contract, and the contract changes, then they are grandfathered from immediately having to have a NACI done - in the near term. If new people join the contract they are subject to the NACI. Eventually, all people will have to have the NACI on file by October 27, 2007, except Federal employees employed for over 15 years which have to have the NACI on file by October 2008.

11. **Is the registrar function required to be performed by a Federal employee or a contractor?**

The Registrar must be a federal employee. However, the Registrar may have a staff consisting of either federal and/or contractor personnel.

12. **Is there a reinvestigation requirement for persons issued a DOE badge but who do not have an access authorization?**

No there is no requirement for a reinvestigation.

13. **What are the records keeping requirements for documents associated with identity proofing process?**

The records keeping requirements are those as specified in FIPS 201.

14. **Can long-term employees, contractors, or visitors awaiting identify proofing be handled as short-term employees, contractors, or visitors until their identity proofing and background checks are completed?**

Yes.

FINGER PRINTS REQUIREMENTS

1. **What are the fingerprinting requirements?**

For PIV-I, the fingerprinting requirement is a full set of fingerprints checked against the FBI National Criminal History database. For PIV-II, an additional requirement will be the capture of a biometric for use with a smartcard. The standard for the biometric has not been finalized.

2. **Is there more information on the FBI's technical requirements?**

Information on the FBI system, Integrated Automated Fingerprint Identification System (IAFIS) is available at http://www.fbi.gov/hq/cjisd/iafis.htm.

3. **Can the fingerprints be taken electronically?**

Yes, using FBI approved equipment. The FBI can process electronic fingerprints much more quickly than processing the paper based fingerprint forms. The IAFIS certified product list is available at http://www.fbi.gov/hq/cjisd/iafis/cert.htm.

ACQUISITION

1. **Is there Department procurement policy for HSPD-12?**

Yes, the Acquisition Letter of July 6, 2005 requires all procurements for HSPD-12 components must be approved through the HSPD-12 program management office.

2. **How will PIV components be procured?**

Some components must be centrally procured; others do not have to be centrally procured, but all must meet PIV interoperability requirements. PIV components will be purchased or approved centrally.

3. **Can you give examples of components that should be centrally procured?**

Smart cards, middleware, and the Identity Management System will be centrally procured .

4. **Can you give examples of components that do not have to be centrally procured?**

A site may want an additional card issuance station. This can be done pending approval from the PMO.

5. **What about Physical Access Control systems?**

If an existing system can be modified or upgraded in a cost effective way, then it will be.

6. **Is there Federal procurement policy for HSPD-12?**

Yes, OMB M-05-24 requires the use of federally approved products and services through GSA.

ACCREDITATION

1. **Who is the Certifying Official?**

The Secretary is required to certify that DOE has implemented PIV-I. This will be done by aggregating the Department and field element Checklists, as prescribed in 206.1.

2. **Is the self-certification requirement contained in DOE Notice 206.1 applicable to those sites whose security clearances are held and processed by other offices?**

The Heads of Departmental and Field Elements are responsible for assuring that sites under their cognizance have implemented 206.1. The Checklist in 206.1 is a signed affirmation that the requirements have been met.